RSAC 2025 Conference

Many Voices. One Community.

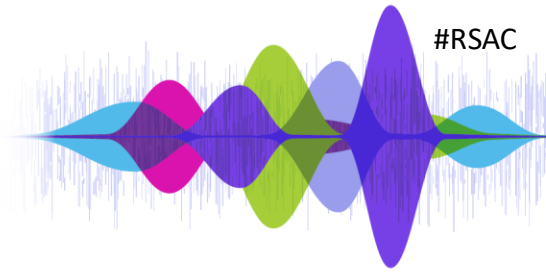
SESSION ID: CTF-M05

Factory Under Siege: Red and Blue Team Tactics in Operational Technology

Nicholas Dhaeyer
Senior OT Analyst
NVISO

Nick Foulon
Senior Security Consultant
NVISO

Sarah Mader
Senior Security Consultant
NVISO



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

WHOAMI

Nicholas Dhaeyer

Senior OT Analyst
at NVISO

Nick Foulon

Senior OT Analyst
at NVISO

Sarah Mader

Red Teamer NVISO
specialized in OT

Agenda

Introduction
How to play the CTF
CTF Time
Lessons Learned & Recap

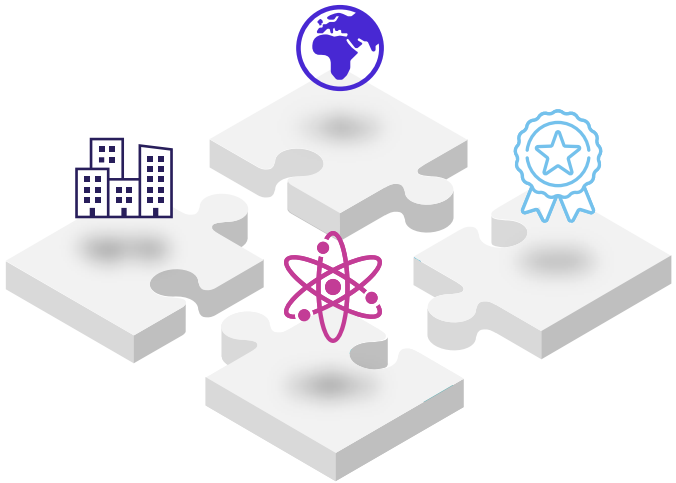
Why should you care?

Worsening Threat Landscape

The worldwide conflicts in Ukraine-Russia, Israel-Hamas, and the South China Sea region encourages adversaries and hacktivists to develop and use new as well as old techniques. As a consequence, threat actors enhance their cyber capabilities.

Integral to Daily Life and Industry

OT is an essential component of modern life, it plays a crucial role in managing the systems that provide us with clean water, regulate traffic flow, healthcare, production of food, and supply electricity.



Regulations

Operational Technology (OT) is regulated through frameworks such as the National Institute of Standards and Technology (NIST) guidelines and the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards.

Increased Connectivity

Many benefits, as greater efficiencies and lower costs, can be achieved with modernization of OT, but this in turn also often increases the attack surface of the environment.

Intro to Operational Technology

"Industrial control systems are used for managing, directing, and regulating the behavior of automated industrial processes. ICS is a term that encompass several types of control systems, but all these systems have some basic traits in common. Their job is to produce a desired outcome, typically maintaining a target state or performing a certain task in an industrial environment."

- SANS.org

The Factory - Purdue Model

The Factory - Purdue Model

Level 3: Operation Systems

e.g. Engineering Workstation, Historian, Jump Host

The Factory - Purdue Model

Level 2: Supervisory Control

e.g. HMI, SCADA

The Factory - Purdue Model

Level 1: Control

e.g. SIS, PLC, RTU

The Factory - Purdue Model

Level 0: Physical Process

e.g. Sensors, Actuators

Red vs. Blue Team

Red Team		Blue Team
Simulates real-world attacks to identify vulnerabilities by attempting to breach security defenses.		Focuses on defending the organization's infrastructure, aiming to protect, detect, and respond to threats.
Enhances security maturity by evaluating people, processes, and technologies for prevention, detection, and response, identifying weaknesses for improvement.		Spreading awareness, strengthening security monitoring, analysing threats, refining incident response strategies and collaborating with other teams to improve defensive measures and resilience.
Offensive, using attacker-like tactics to exploit weaknesses.		Proactive and defensive strategy, focus on people and technology
Works with the White Team, which supervises exercises to ensure effective communication, providing valuable insights for enhancing security.		Collaborates across departments to ensure a comprehensive security strategy, using Red Team insights to enhance protocols.
Uses penetration testing tools and social engineering to simulate attacks.		The Blue Team employs awareness monitoring, analysis, and threat hunting to enhance defensive capabilities.

FACTORY
UNDER SIEGE

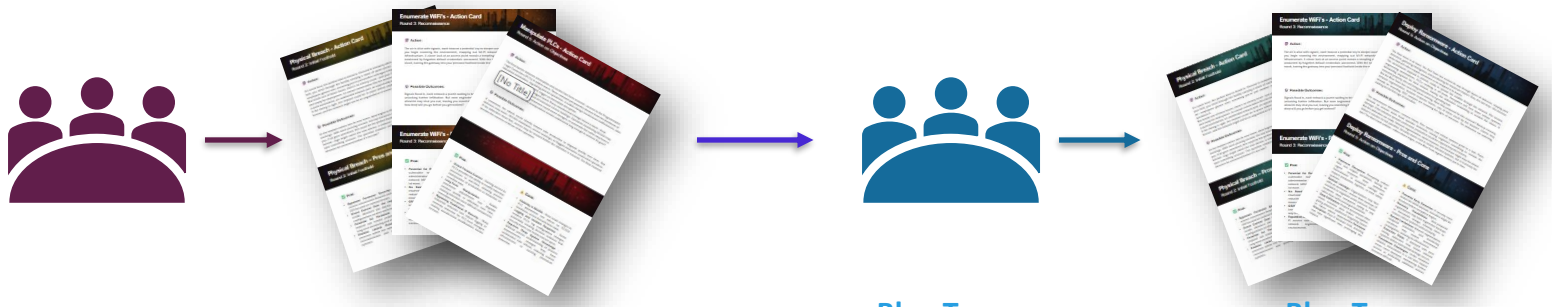
CHOOSE
YOUR TEAM

Game Introduction

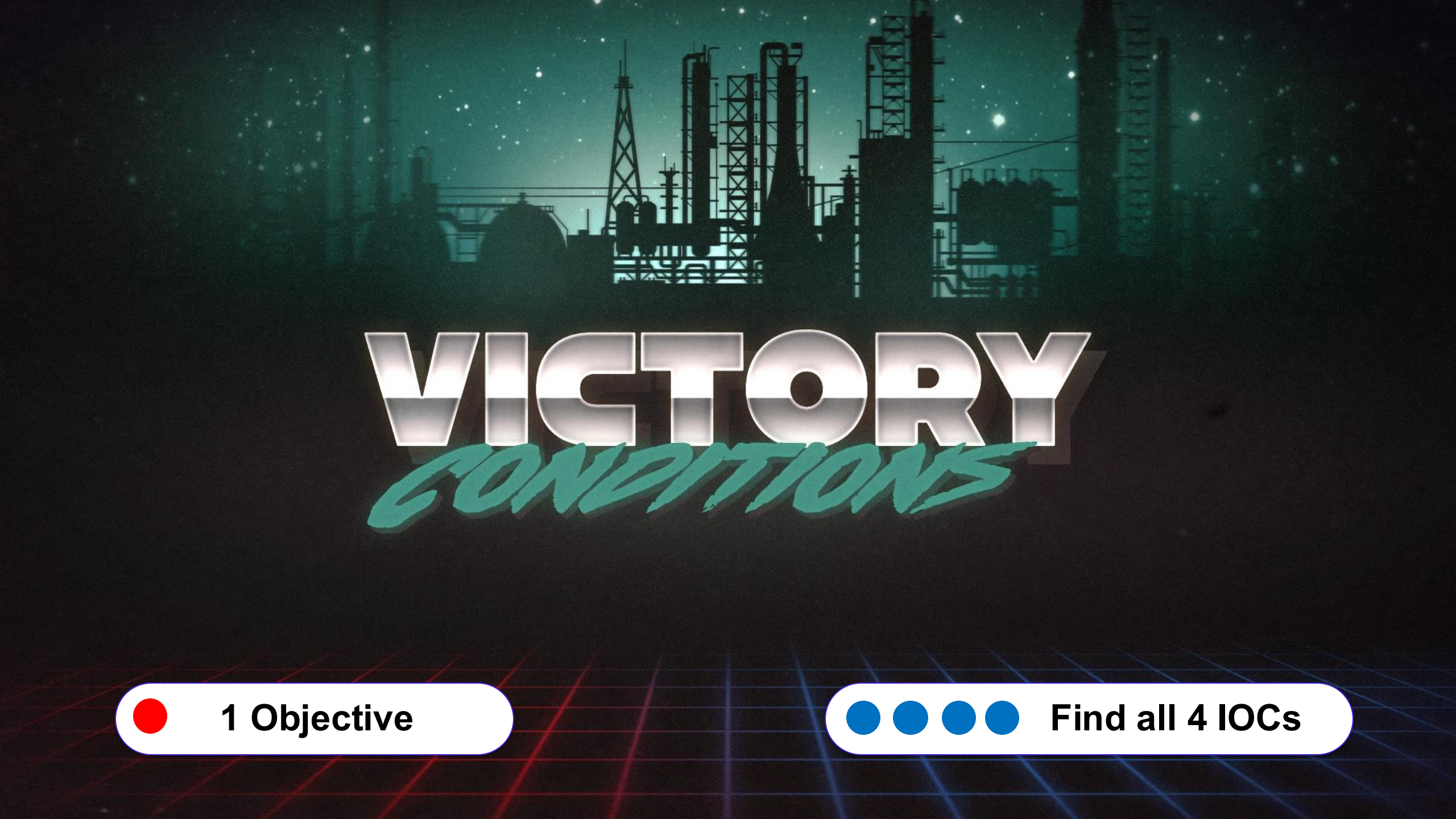
Choose your Weapons → Initial Access → Reconnaissance → Lateral Movement → Showdown

5 Rounds - 60 Minutes

Round



Red Team Discussion → Red Team Action → Alert → Blue Team Discussion → Blue Team Investigation


VICTORY
CONDITIONS
1 Objective
Find all 4 IOCs

RSAC™ 2025 Conference

Let the game begin

CHOOSE
YOUR WEAPONS

INITIAL
ACCESS

RECONNAISSANCE

LATERAL
MOVEMENT

SHOWDOWN

RSAC 2025 Conference

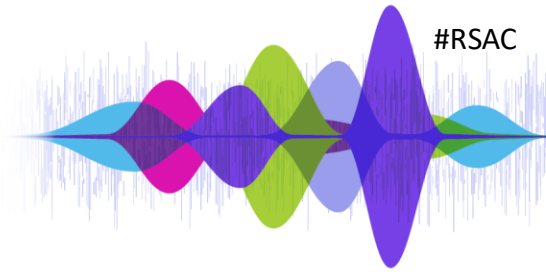
Recap and Lessons Learned

Recap

Choose your Weapons → Initial Access → Reconnaissance → Lateral Movement → Showdown

25 Minutes

What You Have Learned Today



Next Week Reflect

- Think about the Role of Red and Blue Teams in OT Environments
- Reflect on the Decisions made Today by Both Teams

First 3 Month Prepare

- Think how Red and Blue Teams could be used to increase the Security Maturity of a Company
- Identify Stakeholders, Processes & Guidelines involved in an Incident or Red Team

Within 6 months Act

- Start a discussion with Stakeholders to create a Roadmap
- Create a Roadmap on how to assess your OT Environment to detect and remediate Vulnerabilities & Gaps in Incident Response and Detection

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you